



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/993,899	11/24/2001	Helge Bragstad	40.0043	7679
41754	7590	03/20/2006	EXAMINER	
ANDERSON & JANSSON L.L.P. 9501 N. CAPITAL OF TX HWY #202 AUSTIN, TX 78759			KHOSHNOODI, NADIA	
			ART UNIT	PAPER NUMBER
			2137	

DATE MAILED: 03/20/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

## Office Action Summary

Application No.

09/993,899

Applicant(s)

BRAGSTAD ET AL.

Examiner

Nadia Khoshnoodi

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 25 December 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-27 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-27 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 11/24/2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_.

**DETAILED ACTION**

***Response to Amendment***

Applicant's arguments/ amendments with respect to amended claims 1, 10, 15, 19, & 27 and previously presented claims 2-9, 11-14, 16-18, & 20-26 filed 12/27/2005 have been fully considered and therefore the claims are rejected under new grounds. The Examiner would like to point out that this action is made final (See MPEP 706.07a).

The previous objection with regards to the specification is withdrawn due to the amendment filed on 12/27/2005 which supplied a summary for the disclosure.

***Claim Rejections - 35 USC § 103***

I. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

II. Claims 1, 8-10, 17-19, and 26-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Teppler, US Patent No. 6,792,536 and further in view of "Cryptographic Technologies: International Cryptographic Experiment (ICE)".

As per claims 1, 10, 19:

Teppler substantially teaches a method, computer program product, and apparatus for accessing cryptographic material comprising the steps of: creating cryptographic material, by a first Cryptographic-related application programming interface ("API"), in response to a request by a first application compatible with the first Cryptographic-related API (col. 33, lines 6-34).

Not explicitly disclosed is creating a supplemental aspect of the cryptographic material by a supplemental method for the first cryptographic API, wherein the supplemental aspect includes information for rendering the cryptographic material compatible with a second Cryptographic-related API so that the cryptographic material is accessible for a second application by the second Cryptographic-related API. However, SPARTA ISSO teach a translator that is used in order to cure the interoperability issues that arise when using two different cryptographic-related API's that are associated with two different standards. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Teppler for the supplemental aspect to include information for rendering the cryptographic material according to one standard to be compatible with a second Cryptographic-related API that is associated with another standard so that the cryptographic material is accessible for a second application by the second Cryptographic-related API. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since SPARTA ISSO suggest that a translator function is necessary to allow easier development and use of CSP's that are compliant with various CryptoAPI's on page 3, under the heading "Recent Accomplishments" lines 11-20.

Furthermore, as a side note, an article posted on the SPARTA ISSO cite entitled "Security Service API: Cryptographic API Recommendation" (second edition) published in 1996 also supports the notion of using a translator function to cure the interoperability issues that arise when using two different cryptoAPI's that are associated with different standards on page 33 under "Appendix C: Scenarios."

As per claims 8, 17, and 26:

Teppler and SPARTA ISSO substantially teach the method, computer program product, and apparatus of claim 1, 10, and 19. Furthermore, SPARTA ISSO teach wherein the first Cryptographic-related API is one from the set of PKCS #11, CryptoAPI, and CDSA compatible API's, and the second Cryptographic-related API is not the same API as the first and is also one from the set of PKCS #11, CryptoAPI and CDSA compatible API's (page 3, under the heading "Recent Accomplishments" lines 11-20).

As per claims 9, 18, and 27:

Teppler and SPARTA ISSO substantially teach the method, computer program product, and apparatus of claims 1, 10, and 19. Furthermore, SPARTA ISSO teach wherein the first Cryptographic-related API uses a certain term and the second Cryptographic-related API has a corresponding term, and wherein creating the supplemental aspect comprises creating material indicating a cross-reference between the terms (page 3, under the heading "Recent Accomplishments" lines 11-20).

III. Claims 2-7, 11-16, and 20-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Teppler, US Patent No. 6,792,536 and SPARTA ISSO, "Cryptographic Technologies: International Cryptographic Experiment (ICE)" and further in view of Chandrasekaran et al., US Patent No. 6,335,972.

As per claim 2, 11, and 20:

Teppler and SPARTA ISSO et al. substantially teach the method, computer program product, and apparatus of claims 1, 10, and 19. Furthermore, Teppler teaches wherein the step of creating cryptographic material comprises creating a certificate or private key (col. 33, lines 6-

Art Unit: 2137

20). Not explicitly disclosed is the step of creating the supplemental aspect of the cryptographic material comprises the steps of: deriving a key container name from the certificate or private key; and determining whether the key container already exists. However, Chandrasekaran et al. teach generating key recovery fields where if the recovery field exists these fields may be updated. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Teppler for the supplemental aspect to include deriving a key container name from the certificate or private key; and determining whether the key container already exists. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Chandrasekaran et al. suggest that it is important to the functionality of the system to determine if a key container exists or not in response to deriving that key container name from the certificate/private key in col. 15, line 49 – col. 16, line 31.

As per claim 3, 12, and 21:

Teppler, SPARTA ISSO, and Chandrasekaran substantially teach the method, computer program product, and apparatus of claims 2, 11, and 20. Furthermore, Teppler teaches wherein the step of deriving a key container name comprises the steps of: creating a hash responsive to material from the certificate or private key; and encoding the hash (col. 33, lines 35-56).

As per claims 4, 13, and 22:

Teppler, SPARTA ISSO, and Chandrasekaran et al. substantially teach the method, computer program product, and apparatus of claims 2, 11, and 20. Furthermore, Teppler teaches wherein the step of creating a certificate or private key comprises creating the private key (col. 33, lines 6-20). Not explicitly disclosed is wherein if the key container already exists for the key,

Art Unit: 2137

the step of creating the supplemental aspect of the cryptographic material comprises the steps of: determining whether the key container contains a certificate; associating the private key as a member of a key pair associated with the certificate, if the key container contains a certificate; and associating the private key as a member of a key pair having a default key specification, if the key container does not contain a certificate. However, Chandrasekaran et al. teach creating various key recovery fields for keys that exist as well as having a certificate and key recovery contexts for the key. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Teppler to creating the supplemental aspect of the cryptographic material comprises the steps of: determining whether the key container contains a certificate; associating the private key as a member of a key pair associated with the certificate, if the key container contains a certificate; and associating the private key as a member of a key pair having a default key specification, if the key container does not contain a certificate. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Chandrasekaran et al. suggest that there is a need to properly recover keys in order to correctly map them to the correct entity in col. 17, lines 17-36 and col. 18, lines 1-9.

As per claims 5, 14, and 23:

Teppler, SPART ISSO, and Chandrasekaran et al. substantially teach the method, computer program product, and apparatus of claims 2, 11, and 20. Furthermore, Teppler teaches wherein the step of creating a certificate or private key comprises creating the certificate (col. 33, lines 6-20). Not explicitly disclosed is the step of creating the supplemental aspect of the cryptographic material comprises the steps of extracting a key specification from the certificate

Art Unit: 2137

and associating the certificate with a key pair under the extracted key specification. However, Chandrasekaran et al. teach that a profile is created which creates an association with the various certificate chains corresponding to a key pair. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Teppler for creating the supplemental aspect of the cryptographic material to comprise the steps of extracting a key specification from the certificate and associating the certificate with a key pair under the extracted key specification. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Chandrasekaran et al. suggest that there is a need for associating a key pair with a certificate to ensure that an association exists in col. 17, line 54 - col. 18, line 9.

As per claims 6, 15, and 24:

Teppler, SPARTA ISSO, and Chandrasekaran et al. substantially teach the method, computer program product, and apparatus of claims 2, 11, and 20. Furthermore, Teppler teaches wherein the step of creating a certificate or private key comprises creating the certificate (col. 33, lines 6-20). Not explicitly disclosed is wherein if the key container already exists for the certificate the step of creating the supplemental aspect of the cryptographic material comprises the steps of: determining whether the key container has a private key; and associating the private key with a same key pair as the certificate, if the key container has the private key. However, Chandrasekaran et al. teach a profile connected to a key where the key is associated with the certificate chain for the user. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Teppler for the certificate the step of creating the supplemental aspect of the cryptographic material comprises the steps of:

Art Unit: 2137

determining whether the key container has a private key; and associating the private key with a same key pair as the certificate, if the key container has the private key. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Chandrasekaran et al. suggest the importance of ensuring that the private key is mapped to the correct certificate so that the certificate is sure to bind the correct entity with the correct key pair through the certificate in col. 17, line 54 - col. 18, line 9.

As per claims 7, 16, and 25:

Teppler, SPARTA ISSO, and Chandrasekaran et al. substantially teach the method, computer program product, and apparatus of claims 2, 11, and 20. Furthermore, Teppler teaches wherein the step of creating a certificate or private key comprises creating the certificate (col. 33, lines 6-20). Not explicitly disclosed is the step of creating the supplemental aspect of the cryptographic material comprises the step of: creating a public key from information in the certificate. However, Chandrasekaran et al. teaches that a public key certificate chain is comprised in the profile for the key recovery system. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Teppler for the step of creating the supplemental aspect of the cryptographic material comprises the step of: creating a public key from information in the certificate. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Chandrasekaran et al. suggests that there must be a public key to a public-private key pair to allow decryption to take place to validate the source in col. 17, line 54 - col. 18, line 9.

*\*References Cited, Not Used*

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

1. US Patent No. 6,385,729
2. US Patent No. 6,772,341
3. US Patent No. 6,484,259
4. US Patent No. 5,996,076
5. Balenson, David: "International Cryptography Experiment (ICE)"
6. NSA Cross Org. CAPI Team: "Security Service API: Cryptographic API Recommendation "
7. NSA Cross Org. CAPI Team: "Security Service API: Cryptographic API Recommendation"  
(2<sup>nd</sup> Edition)

The above references have been cited because they are relevant due to the manner in which the invention has been claimed.

***Conclusion***

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a).

Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).


A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

Art Unit: 2137


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825.

The examiner can normally be reached on M-F: 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

  
Nadia Khoshnoodi  
Examiner  
Art Unit 2137  
3/16/2006

NK

  
EMMANUEL L. MOISE  
SUPERVISORY PATENT EXAMINER